


IN THE UNITED STATES PATENT AND TRADEMARK OFFICE



In re application of: Arturo Maria

Application No. 09/580,689

Filed: May 30, 2000

Confirmation No. 1763

For: FLOATING INTRUSION DETECTION
PLATFORMS

Examiner: Carl G. Colin

Art Unit: 2785

Attorney Reference No. 6541-62119-01

CERTIFICATE OF MAILING

I hereby certify that this paper and the documents referred to as being attached or enclosed herewith are being deposited with the United States Postal Service as First Class Mail in an envelope addressed to: MAIL STOP AMENDMENT, COMMISSIONER FOR PATENTS, P.O. BOX 1450, ALEXANDRIA, VA 22313-1450 on the date shown below.

Attorney or Agent
for Applicant(s)



Date Mailed June 13, 2005

MAIL STOP AMENDMENT
COMMISSIONER FOR PATENTS
P.O. BOX 1450
ALEXANDRIA, VA 22313-1450

DECLARATION UNDER 37 C.F.R. § 1.131

Dear Sir:

I, Michael D. Jones, declare that copies of the following documents pertaining to U.S. Patent Application 09/580,689, filed May 30, 2005 and naming Arturo Maria as inventor are attached:

1. An Invention Disclosure for Patent Review dated December 10, 1998, naming Art Maria as submitter;
2. A letter, dated November 11, 1999, requesting preparation of a patent application for "Floating Intrusion Detection Machines (FIDM)," Arturo Maria, inventor;
3. A letter, dated April 10, 2000, enclosing a draft patent application stating that the application has been reviewed and approved by the inventor, Arturo Maria, and is enclosed for additional review;

4. A letter, dated May 5, 2000, enclosing a patent application reviewed and approved by the inventor, Arturo Maria, as well as by AT&T; and
5. A letter to Mr. A. Maria, dated May 9, 2000, enclosing a copy of a patent application ready to be filed and a Declaration and Power of Attorney for signature by Mr. Maria.

Respectfully submitted,

KLARQUIST SPARKMAN, LLP

By



Michael D. Jones
Registration No. 41,879

One World Trade Center, Suite 1600
121 S.W. Salmon Street
Portland, Oregon 97204
Telephone: (503) 226-7391
Facsimile: (503) 228-9446



BEST AVAILABLE COPY

AT&T Wireless Services

Invention Disclosure for Patent Review

Page 1 of 2

Revision 12/10/98

Note: To use this form online, tab or arrow-key between fields; press the space bar to check boxes.

Date: 12/10/98

Submitter's Name: Art Maria

Submitter's Phone:

E-mail Address:

Please answer the following as completely as possible. If you already have a document that describes your idea, attach it along with this form.

Title of Your Idea

Floating Intrusion Detection Machines (FIDM)

Brief Description

When describing your idea, please address the following:

- What is it?
- How does it work?
- Describe if there is a date involved, e.g., introduction or announcement of a service or product.

Intrusion Detection Systems (IDS) are commonly known hardware/software systems which use knowledge based rules and artificial intelligence concepts to detect patterns of attacks in network systems. These patterns of attacks are usually stored in profiling databases.

IDS platforms are usually placed at critical network entry points; as network packets enter the network, these packets are inspected by IDS sensors, and compared against profiles stored in databases for potential rejection and alarming.

This invention describes a Floating Intrusion Detection Machine (FIDM) architecture which is a unique software system comprised of four elements: (a) FIDM sensors, (b) servers, (c) sockets and (d) machines.

(a) FIDM Sensors: Intrusion Detection Systems (IDS) platforms which use centralized FIDM servers and databases to detect and filter attacks.

(b) FIDM Servers: IDS database servers which host knowledge-based rules and patterns of attacks.

(c) FIDM Sockets: Software programs and reserved areas which have the ability to host FIDM software agents transmitted through the network. When software agents are received, these sockets host the programs and commence execution of the code which takes over the machine and convert the machine into an FIDM platform.

(d) FIDM Machines: Any machine in the network capable of hosting FIDM sockets and agents. Once the agent is loaded, the FIDM machine is transformed into an FIDM sensor or server.

The primary benefit of the FIDM architecture is the capability to implement network elements that would take control over "any" machine in a network designated as FIDM capable, and convert this device into an Intrusion Detection System (IDS) sensor or server depending on particular real-time needs. The invention works as follows:

FIDM sensors would be placed at the perimeter entrances of network(s) being protected.

FIDM servers would be placed in protected or "bastion" sub-networks. These servers would host centralized knowledge base rules databases which would contain historical patterns of attack.

In addition to the FIDM server, there would be an unlimited number of machines that would be designated as FIDM platforms. Each FIDM platform would have the potential of being converted into an FIDM sensor and/or server in the event of a network attack.

Machines designated as potential FIDM platforms in the network would have an FIDM "socket" installed in the TCP/IP network stack. When a network intrusion would be detected, the FIDM server would attach an FIDM agent to the machine being designated as the new FIDM sensor/server. This agent would take control over the machine and transform the machine into an FIDM sensor or server depending on the particular intrusion detected.

Since every host in the network is a potential FIDM sensor/filter, intruders would be hard pressed to devise strategies to bypass or compromise Intrusion Detection Systems.

Another advantage of this architecture is that sensors and servers do not have to be pre-assigned in the network. The only preassignment would have to take place in the initial FIDM server and associated databases. Once the client socket is installed in potential FIDM platforms, any of these machines could be transformed into an IDS sensor, filter or server depending on the need.

BEST AVAILABLE COPY

Invention Disclosure for Patent Review Form

Page 2 of 2

Objective

Use the following questions as guides to help you complete this section:

- What problem does this idea solve or what purpose does it serve?

The primary benefit of the FIDM architecture is the capability to implement network elements that would take control over "any" machine in a network designated as FIDM capable, and convert this device into an Intrusion Detection System (IDS) sensor or server depending on particular real-time needs.

Comparison

Use the following as guides to help you complete this section:

- Describe any related work of which you are aware, e.g. past publications or other products.
- How is your idea different from what's been done before?
- What commercial benefits are derived from these differences?

Use

Submitters

Include yourself and any others who collaborated with you in the development of this idea as "co-inventors."

You:

Name:

Art Maria

Full Home Address:
(including county)

Manager:

Co-Inventor 1:



BEST AVAILABLE COPY



November 11, 1999

Kenyon and Kenyon
1500 K. Street, NW
Washington, DC 20005

Dear:

Please prepare a formal patent application for the attached disclosure.

IDS No. 113639, AWS 459

Inventors: Arturo Maria
Work 425 580 6162
2802 107th Avenue NE
Bellevue, WA 98004
Email: art.maria@attws.com

Title: Floating Intrusion Detection Machines (FIDM)

BEST AVAILABLE COPY

LAW OFFICES OF
KENYON & KENYON
1500 K STREET, N.W., SUITE 700
WASHINGTON, D.C. 20005-1257
TEL. (202) 220-4200
FAX. (202) 220-4201

NEW YORK OFFICE
ONE BROADWAY
NEW YORK, N.Y. 10004-1000
TEL. (212) 425-7800
FAX. (212) 425-8258

SILICON VALLEY OFFICE
RIVERPARK TOWERS, SUITE 600
333 W. SAN CARLOS ST.
SAN JOSE, CA 95110-2731
TEL. (408) 975-7800
FAX. (408) 975-7501

FRANKFURT OFFICE
SCHILLERSTRASSE 19-25
60313 FRANKFURT AM MAIN
FEDERAL REPUBLIC OF GERMANY
TEL. (49) (69) 97 55 05 0
FAX. (49) (69) 97 55 05 99

WWW.KENYON.COM

April 10, 2000

VIA Two Day Priority

AT&T Corp.
200 Laurel Avenue
Room E43B12
Middletown, NJ 07748

Re: **U.S. Patent Application**
FLOATING INTRUSION DETECTION PLATFORMS
Your Ref. AWS 459, IDS 113639; Our Ref.: 2685/113639

Dear :

Please find enclosed for AT&T's review the draft application prepared by us for the above referenced case. It has already been reviewed and approved by the inventor, Arturo Maria.

Sincerely,

KENYON & KENYON

Enclosure

BEST AVAILABLE COPY

LAW OFFICES OF
KENYON & KENYON
1500 K STREET, N.W., SUITE 700
WASHINGTON, D.C. 20005-1257
TEL. (202) 220-4200
FAX. (202) 220-4201

NEW YORK OFFICE
ONE BROADWAY
NEW YORK, N.Y. 10004-1090
TEL. (212) 485-7500
FAX. (212) 485-8288

SILICON VALLEY OFFICE
RIVERPARK TOWERS, SUITE 600
333 W. SAN CARLOS ST.
SAN JOSE, CA 95110-8731
TEL. (408) 975-7500
FAX. (408) 975-7501

FRANKFURT OFFICE
SCHILLERSTRASSE 19-25
60313 FRANKFURT AM MAIN
FEDERAL REPUBLIC OF GERMANY
TEL. (49) (69) 97 55 05 0
FAX. (49) (69) 97 55 05 99

WWW.KENYON.COM

May 5, 2000

VIA Two Day Priority

AT&T Corp.
200 Laurel Avenue
Room E43B12
Middletown, NJ 07748

Re: U.S. Patent Application
FLOATING INTRUSION DETECTION PLATFORMS
Your Ref: AWS 459, IDS 113639; Our Ref.: 2685/113639

Dear :

Please find enclosed an application prepared by us for the above referenced case which is ready to be filed, as well as a form PTO-1449, with copies of the cited references. The application has already been reviewed and approved by the inventor, Arturo Maria, as well as by AT&T.

Sincerely,

KENYON & KENYON

Enclosure

BEST AVAILABLE COPY



May 9, 2000

Mr. A. Maria

Dear Mr. Maria:

RE: Docket No. 113639 (AWS 459)
Floating Intrusion Detection Platforms

Enclosed is a copy of the above-identified patent application that is ready to be filed in the U.S. Patent Office. Also enclosed is the formal document you must sign in order to complete the patent filing requirements.

After reviewing the application, please read the Declaration and Power of Attorney and then sign and date it—in blue ink as your name is typed—at the appropriate place on the document. (No notarization is required.) Please return the signed document to me as soon as possible.

BEST AVAILABLE COPY

Sincerely,

**Atts.
As stated**